REMARKS

Applicant has amended the claims to overcome the objection raised to claims 22-24 and to overcome the objection in claims 21-27. In doing so, applicant has added new claims 40-56. Applicant now believes claims 21-27 complies with 37 CFR 1.75(c) in that none of the claims depend from another multiple dependent claim.

The rejection of claim 39 under 3 USC 101 is respectfully traversed. Applicant has amended claim 39 to specify that the computer program is stored in memory executable in the reception equipment. Accordingly, applicant believes the rejection under 35 USC 101 should be withdrawn.

The rejection of claims 22-24 under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention, is respectfully traversed.

The applicant respectfully points out that claims 22-24 do not represent computer code instructions as suggested by the Examiner. Instead, these claims describe a format of data transmitted to reception equipment in EMM messages that represent the list of M identifiers of the external security module or modules and the structure of the commands to carry out the check phase. Applicant does not believe the description of this format in claims 22-24 is unclear, but instead represents limitations of exactly how to transmit the data to the reception equipment. Accordingly, the rejection of claims 22-24 should be withdraw.

The rejection of claims 1-20, 38 and 39 under 35 USC 103(a) as being unpatentable over Hirota (USP 6,606,707) and further in view of Tsuria (USP 6,405,369) is respectfully traversed.

Claim 1 has been amended to clearly define the subject matter which the

applicant regards as the invention.

This invention is directed to a method for matching a number N of data reception equipment with a number M of external security modules, each reception equipment being provided with a unique identifier, and each external security module having a unique identifier. This method comprises the following steps:

a- memorizing a list of identifiers of different reception equipment in each external security module,

b- memorizing a list of identifiers of different external security modules in each reception equipment,

when an external security module is connected to a reception equipment, a check phase is carried out to:

c- verify whether or not the identifier of said connected external security module is present in the list memorized in said reception equipment, and whether or not the identifier of said connected reception equipment is present in the list memorized in said external security module,

d- and, if so, authorizing access to data using said external security module and said reception equipment,

e- and, if not, preventing access to the distributed data by means of said external security module with said reception equipment.

Neither Hirota, nor Tsuria discloses or suggests the steps of: (1) memorizing a

list of identifiers of reception equipment in each external security module and (2) memorizing a list of identifiers of external security module in each reception equipment nor teach carrying out a phase check when an external security module is connected to said reception equipment for verifying whether or not the identifier of an external security module connected to reception equipment is present in the list memorized in the connected reception equipment, and whether or not the identifier of said reception equipment is present in the list memorized in said connected external security module as is claimed in claim 1.

Hirota concerns a semiconductor memory card comprising an authentication area for storing copyright protected digital contents and a non-authentication area for storing other data.

The semiconductor memory of Hirota further comprises an authentication unit to manage access to the authentication area. *At col.5, lines 9-17, Hirota recites*:" In the above semiconductor memory card, the authentication unit may request a user of the electronic device to input a user key, which is information unique to the user, during the authentication process, and the control circuit further includes: a user key storage unit which stores the user key; an identification information identifying an electronic device that has been affirmatively authenticated by the authentication unit"

Hirota is not concerned with matching a number N of data reception equipment with a number M of external security modules in order to allow access to digital data by means of different external security modules matched with different reception equipment.

Tsuria relates to a method for activating the decoding of pay television transmissions in a second decoder when said pay television transmissions are already decoded by a first smart card in a first decoder (see col. 1, lines 61-65).

The decoding by the second smart card in the second decoder is possible only if there is a correspondence between one of, signature, a key and a seed identifying the first smart card and a corresponding one of signature, a key and a seed identifying the second smart card (see col. 3, lines 1-5).

Tsuria does not relate to the method of matching a number N of data reception equipment with a number M of external security modules in order to allow access to digital data by means of different external security modules matched with different reception equipments. Moreover, Tsuria does not teach or suggest (1) memorizing a list of identifiers of reception equipments in each external security module and (2) memorizing a list of identifiers of external security modules in each reception equipment and does not carry out a phase check when an external security module is connected to reception equipment for verifying whether or not the identifier of said external security module is present in the list memorized in said reception equipment, and whether or not the identifier of said reception equipment is present in the list memorized in said external security module.

Moreover, Tsuria requires the practice of critical conditions not present in the subject invention to verify correspondence between the second smart card in the second decoder with a specific signature or key of the first smart card.

CONCLUSION

For all of the above reasons, claims 1-39 are now believed to be clearly patentable over the cited prior art, whether taken individually or in combination and the rejection under 35 USC 103 should be withdrawn.

Claims 40-56 are dependent claim which are believed to be patentable for the same reasons as given above.

Reconsideration and allowance of claims 1-56 is respectfully solicited.

Respectfully submitted,

Eugene Lieberstein
Reg. No. 24,645

Customer # 79681
BAKER & HOSTETLER LLP
45 Rockefeller Plaza
New York, NY 10111
Tel: 212-589-4634
Fax: 212-589-4201

MAILING CERTIFICATE

I hereby certify that this correspondence is being sent to the USPTO via EFS Web to the Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450, on 10/13/10.

By L. Quaglariello